REMARKS

The Applicant has reviewed the Official Action, mailed May 9, 2002, and has prepared this Amendment in response thereto. The application has been amended to include an abstract and to amend the format of the specification in accordance with U.S. rules of practice. No new matter has been added. Claims 1 - 12 were amended to correct the errors identified in the Examiner's objection, and claims 1, 5 and 6 were amended in response to the rejections under 35 USC §102. Claims 1 – 12 remain in the application. In support of the Applicant's assertion that the claims, as amended, are novel and unobvious, the Applicant has submitted the Declarations Under 37 CFR §1.132 of Dr. Mongi Abidi, Dr. Hideki Noda, and Dr. Kyoki Imamura, each of whom are experts in the field of the present invention.

The following remarks will follow the sequence set forth in the Official Action.

Objections to the Specification

In response to the Examiner's objections, the Applicant has added an Abstract and has amended the specification to correct the format to conform to U.S. practice. It is noted that the original application was filed in Japan and, therefore, was drafted to conform to Japanese practice. This application was amended during the international phase of the PCT, but the original application, as published by WIPO, was filed as a U.S. national application under 35 USC §119. The attached amendments to the specification merely alter the format of the specification and do not add any new matter.

Claim Objections

Claims 1-4 and 6 - 12 were objected to based upon obvious errors pointed out by the Examiner. In response, the Applicant has amended these claims in accordance with the Examiner's

helpful suggestions. Accordingly, the Applicant respectfully requests that these objections be withdrawn.

Claim Rejections – 35 USC §102

Claims 1 - 12 were rejected under 35 U.S.C. §102 as anticipated by the Rhoads reference. The Applicant respectfully disagrees with this rejection on the grounds that the Rhoads reference fails to disclose or suggest an information card comprising a memory, which is affirmatively claimed in each of claims 1 - 20. This lack of disclosure or suggestion of a memory was acknowledged by the European Patent Office in its International Preliminary Examination Report, a copy of which was filed concurrent with the present application, which required the use of an additional reference in its rejection to show a memory. It is noted that the Examiner did not refer to any memory in his rejection and, therefore, may not have accorded the memory limitation any patentable weight. However, the Applicants clearly intended the memory to be an affirmative limitation, as evidenced by the EPO's reading of it as such in its Report. Therefore, it is respectfully requested that the memory limitation be accorded patentable weight and that the rejections under 35 USC §102 be reconsidered and withdrawn.

Nonobviousness of claims 1 - 20

In response to an anticipated obviousness rejection of claim 1 based upon 35 USC §103, the Applicant has amended claims 1 and 5 to include the limitation that the "inherent data authenticates the legitimacy of a card owner of the information card". This limitation was originally set forth in claim 2, which has been amended to eliminate this limitation via the attached amendment. For the reasons set forth below, the undersigned believes that the claims, as amended, are novel and unobvious over the cited art, both alone and in combination.

MPEP §2142 states that "(t)o establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references must teach or suggest all of the claim limitations." The Applicants assert that at least the first of these requirements has not been met.

The Rhoads reference cited in the rejection is titled "STEGANOGRAPHY METHODS EMPLOYING EMBEDDED CALIBRATION DATA" and discloses methods of embedding data that "are characterized by robustness despite degradation of the encoded carrier, and by permeation of the identification signal throughout the carrier." (See Rhoads, abstract, lines 5 - 7). Such methods are said to include a "method for performing a positive identification between a copy of an original signal and the original." (See Rhoads, column 3, lines 18 - 20), with the principal purpose of providing a deterrent to piracy. The methods function as a deterrent as they are said to "(a) cost effectively monitor for unauthorized uses of material and perform "quick checks"...(c) provide unequivocal proof of identity, similar to fingerprint identification, in litigation, with potentially more reliability than that of fingerprinting." (See Rhoads, column 3, lines 34-36, & 38 - 40). Accordingly, the Applicant asserts that the methods disclosed in the Rhoads reference are primarily directed to the authentication of the identity of a signal, computer file, image, card, or the like, rather than the authentication that the holder of such a signal, computer file, image or card is the rightful owner, and that there would be no motivation to modify the Rhoads methods to authenticate that the holder of such a signal, computer file, image or card is the rightful owner.

The Applicants' assertion is supported by the Declarations Under 37 CFR §1.132 of Dr.

Mongi Abidi, Dr. Hideki Noda, and Dr. Kyoki Imamura, each of whom are persons of at least ordinary skill in the relevant art. Each Declarant declares that the "methods disclosed in the Rhoads reference are primarily directed to the authentication of the identity of a signal, computer file, image, card, or the like." Further, the Declarants each declare that "based upon the teachings of Rhoads, I would have no motivation to modify the Rhoads methods to authenticate that the holder of such a signal, computer file, image or card is the rightful owner."

In the embodiment cited by the Examiner (see Rhoads FIGS. 22 - 26, and from column 57, line 30, to column 61, line 47), "PLASTIC CREDIT AND DEBIT CARD SYSTEMS BASED UPON THE PRINCIPALS OF THE INVENTION" are disclosed. The basic principles of these methods are set forth at column 58, lines 17-45 of Rhoads, which reads as follows:

> "The short story is that the personal cash card 950 actually contains a very large amount of information unique to that particular card. There are no magnetic strips involved, though the same principles can certainly be applied to magnetic strips, such as an implanted magnetic noise signal (see earlier discussion on the "fingerprinting" of magnetic ships in credit cards; here, the fingerprinting would be prominent and proactive as opposed to passive). In any event, the unique information within the image on the personal cash card 950 is stored along with the basic account information in a central accounting network, 980, FIG. 26. The basis for unbreakable security is that during transactions, the central network need only query a small fraction of the total information contained on the card, and never needs to query the same precise information on any two transactions. Hundreds if not thousands or even tens of thousands of unique and secure "transaction tokens" are contained within a single personal cash card. Would-be pirates who went so far as to pick off transmissions of either encrypted or even unencrypted transactions would find the information useless thereafter. This is in marked distinction to systems which have a single complex and complete "key" (generally encrypted) which needs to be accessed, in its entirety, over and over again. The personal cash card on the other hand contains thousands of separate and secure keys which can be used once, within milliseconds of time, then forever thrown away (as it were). The central network 980 keeps track of the keys and knows which have been used and which haven't."

The "transaction tokens" that interact with the central network are formed by placing a

"master snowy image" over a user's image, which produces the master image that is printed on the card. "The overall effect on the image is to "texturize" the image." (Rhoads, column 59, line 35-36). As an additional safeguard against fraud, the card also is said to provide "PIN security and the user picture security (a known higher security than low wage clerks analyzing signatures). " (Rhoads, column 61, lines 39-41). However, it is acknowledged that a thief having access to photo-quality copying devices may copy the card. (See Rhoads, column 61, lines 41-43)

As described in the above cited passages, credit and debit cards utilizing the methods disclosed in Rhoads may be effective at determining that a particular card is not a "phony" or a "crude reproduction" of a true original card. However, it has significant drawbacks that make it unsuited to succeed in solving one key problem set forth by the Applicants of the present application, namely the provision of an "information card, which can completely be prevented from being illegally used, and a n information card system." (See Objects of the Invention, page 3, lines 9 – 11).

First, the card disclosed in Rhoads does not provide any authentication that the user of the card is the owner of the card. Rather, user authentication is left to the same "low wage clerks" who were said to be unable to adequately analyze signatures. Thus, the card disclosed in Rhoads does not include the "inherent data that authenticates the legitimacy of a card owner of the information card", which is claimed by the Applicant.

Second, the system contemplated by Rhoads performs all processing at the central network and not at a data processing terminal. This is said to be preferred as the information read from the card is not transmitted, but rather a twenty-four dot product, based upon the random numbers generated by the network and the information upon the card, is transmitted to the network, which authenticates the card and sends only an approval to the data processing terminal. (See Rhoads, FIG. 25 and between

column 60, line 39, to column 61, line 31). Given the authentication method disclosed, the card system of Rhoads does not include any "output means for outputting the read information data", as claimed in claims 5 - 12. Further, because the system is specifically designed to avoid a transmission of the actual data, there would be no motivation to modify the system of Rhoads to include such an "output means".

These assertions are likewise supported by the three attached Declarations, with each Declarant declaring that "the card disclosed in the Rhoads reference does not provide any authentication that the user of the card is the owner of the card and does not include any "output means for outputting the read information data", as claimed in the Applicant's claims 5 - 12. " Each further declares "that, because the system disclosed in the Rhoads is specifically designed to avoid a transmission of the actual data, I would have no motivation to modify the system to include such an "output means"."

Third, the card system of Rhoads must be used with a network terminal and, accordingly, may not be used in locations that do not have telecommunications access. Conversely, the embodiments of the Applicants' card system claimed in claims 5 – 12 and 15 – 20, may be utilized as a "stand alone" system that simply utilizes the information hidden within the card to provide authentication of the user.

The assertion is likewise supported by the three attached Declarations, with each Declarant declaring that "the card system disclosed in the Rhoads reference must be used with a network terminal and may not be used in locations that do not have telecommunications access" and that they "would have no motivation to modify the system of Rhoads to obtain a "stand alone" system that simply utilizes the information hidden within the card to provide authentication of the user, as claimed by the Applicant."

For the reasons set forth above, the undersigned asserts that the Rhoads fails to disclose or

suggest a card system that includes "inherent data that authenticates the legitimacy of a card owner of the information card", as claimed in independent claims 1 and 5. Further, Rhoads fails to disclose or suggest a card system having a data processing terminal that includes "an output means for outputting the extracted inherent data", as claimed in claims 5 – 12 and 15 - 20, as amended. Accordingly, the undersigned asserts that claims 1 – 20 are both novel and unobvious in light of Rhoads, both alone and in combination with the art cited by the Examiner and during the International Phase of the PCT, and respectfully requests that all claims be reconsidered and allowed.

Conclusion

It is felt that a full and complete response has been made to the Official Action and, as such, places the application in condition for allowance. Such allowance is hereby respectfully requested. If the Examiner feels, for any reason, that a personal interview will expedite the prosecution of this application, he is invited to phone applicant's attorney.

Respectfully submitted,

Date September 9, 2002

Michael J. Persson
Attorney for Applicant
Registration No. 41,248
Lawson, Philpot & Persson, P.C.
67 Water Street, Suite 110
Laconia, NH 03246
Phone: 603-528-2900
Fax: 603-528-1117

Claims 1 - 12, with indicia of amendment

1. ~~In~~ An information card ~~including~~ comprising a memory that stores information data, the information data ~~including~~ comprising one of image data and acoustic data~~,~~; ~~the improvement~~ wherein the information data contains inherent data that is embedded in the information data according to ~~Steganography~~ steganographic information hiding; and

wherein the inherent data comprises data that authenticates a legitimacy of a card owner of the information card.

2. ~~An~~ The information card according to claim 1, wherein the inherent data ~~shows one of~~ further comprises data that authenticates a legitimacy of the information card.

3. ~~An~~ The information card according to claim 1 ~~or 2~~ wherein the memory stores a password for permitting the information data to be read from the memory.

4. ~~An~~ The information card ~~according to any one of claims 1 to 3~~ claim 1, wherein the information card employs a customized key in order to give a permission to extract the inherent data from the information data.

5. An information card system comprising:

an information card ~~including~~ comprising a memory that stores information data, the information data comprising one of image data and acoustic data, wherein the information data ~~including~~ comprises inherent data that is embedded in the information data according to ~~Steganography~~ steganographic information hiding, wherein the inherent data comprises data that authenticates a legitimacy of a card owner of the information card, and wherein the memory stores ~~storing~~ a password for permitting the information data to be read from the memory; and~~,~~

a data processing terminal ~~including~~ comprising input means for submitting a password, password checking means for checking the submitted password against the password stored in the information card to permit the information data to be read from the memory, and output means for outputting the read information data.

6. An information card system comprising:

an information card ~~including~~ comprising a memory that stores information data, wherein the information data ~~including~~ comprises one of image data and acoustic data, wherein the information data ~~including~~ comprises inherent data that is embedded in the information data according to ~~Steganography~~ steganographic information hiding; and,

a data processing terminal ~~including~~ comprising input means for submitting a customized key, inherent data extracting means for extracting the inherent data with the use of the submitted customized key, and output means for outputting the extracted inherent data.

7. ~~An~~ The information card system according to claim 6, wherein the memory stores a password for permitting the information data to be read from the memory, and wherein the data processing terminal ~~includes~~ comprises input means for submitting a password, password checking means for checking the submitted password against the password stored in the information card to permit the information data to be read from the memory, and output means for outputting the read information data.

8. ~~An~~ The information card system according to ~~any one of claims 5 to 7~~ claim 7, wherein the extracted inherent data is ~~wholly or~~ at least partly checked against one of inherent data read from a host and inherent data entered from an external source.

9. ~~An~~ The information card system according to claim 6, ~~any one of claims 1 to 8~~ ,

wherein the inherent data is embedded according to Steganography by the steps of

wherein said system further comprises a means for embedding the inherent data, said means for embedding comprising:

at least one of a means for converting one of image data and acoustic data~~, both formed as information data,~~ to pure binary code data, and a means for ~~or~~ converting the pure binary code data to canonical gray code data~~;~~;

means for decomposing one of the pure binary code data and the canonical gray code data into bit planes;

means for segmenting the bit planes into regions according to a complexity measure, and

means for replacing complex region-forming data with the inherent data.

10. ~~An~~ The information card system according to claim 9, wherein the ~~inherent data to be embedded is subject to a conjugation operation~~ means for embedding the inherent data further comprises means for performing a conjugation operation upon the inherent data.

11. ~~An~~ The information card system according to claim 6 ~~any one of claims 1 to 10~~, wherein the memory comprises an ~~IC~~ integrated circuit chip.

12. ~~An~~ The information card system according to claim 6 ~~any one of claims 1 to 11~~, wherein the information card carries a photograph on a surface thereof, and one of the information data and the inherent data is image data representing the photograph.